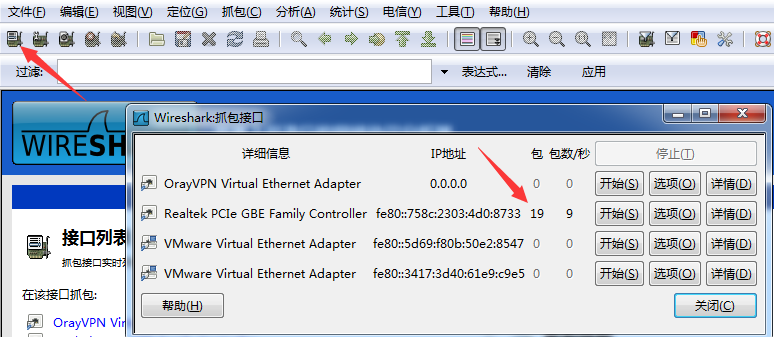
1. **关于邮件白名单：**

①打开Wireshark，然后先选择需要监控的网卡信息，比如我用的是本地网卡进行上网：



②如果不清楚是哪张网卡的话，可以点这个按钮，看下哪个网卡有数据在走，就选择这个网卡，如图：

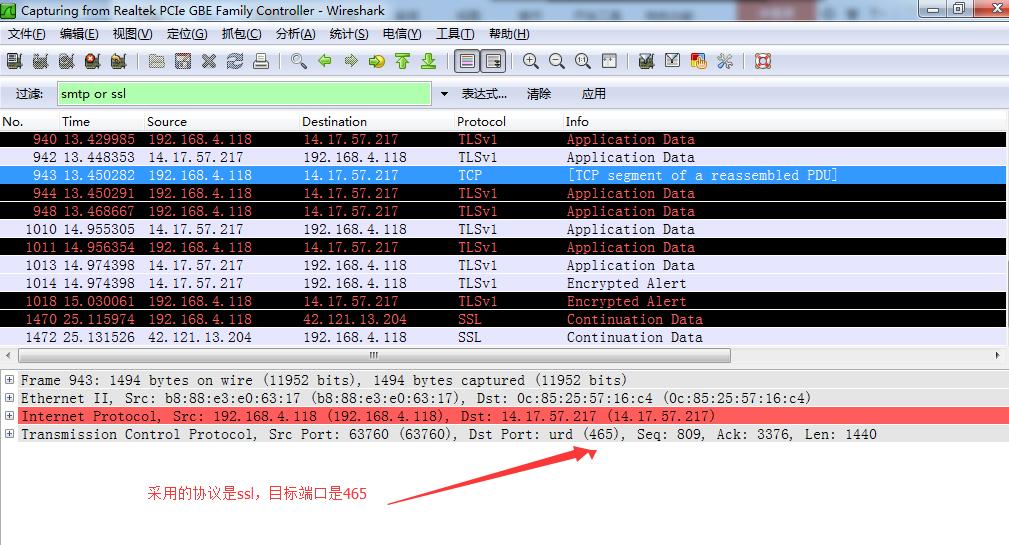


③选择完网卡，之后我们就要检查下发送邮件采用的是smtp协议还是采用的是ssl协议，需要再过滤器那边设置下过滤，关键字是： smtp or ssl，然后回车之后就可以发送邮件，抓取数据包了，如下图：

**下面是163邮箱的，是smtp协议的，这个我们就可以支持：**



**下面是公司企业邮箱，是ssl协议，这个我们不能支持：**



**以上就是关于邮件协议的监控。**

1. **关于服务器白名单监控**

比如我要监控一个oa的协议是什么，我可以输入关键字：

**ip.addr==192.168.1.230**